Quantum Computation - Lecture 07 - Quantum Error Correction I

Mateus de Oliveira Oliveira

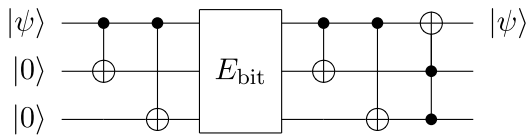
TCS-KTH

January 20, 2013

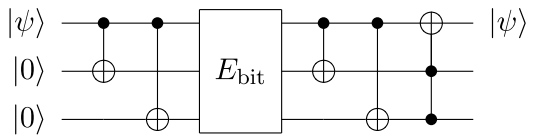
- No cloning theorem

- No cloning theorem
- Errrors are continuous

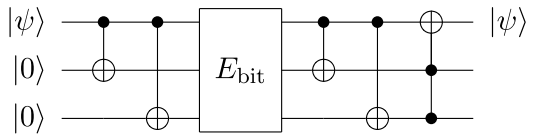
- No cloning theorem
- Errrors are continuous
- Measurements destroys information



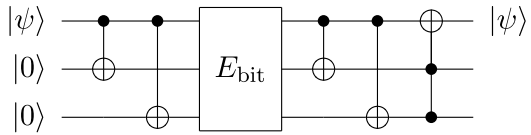
- The Code:



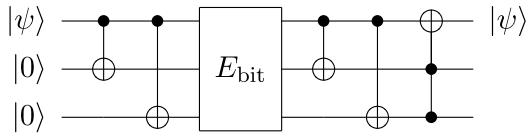
- The Code:
  - $|0\rangle \rightarrow |000\rangle$



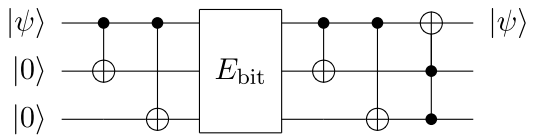
- The Code:
  - $|0\rangle \rightarrow |000\rangle$
  - $|1\rangle \rightarrow |111\rangle$



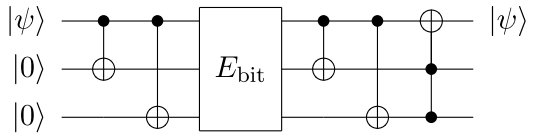
- Syndrome detection:



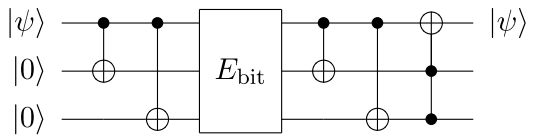
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.



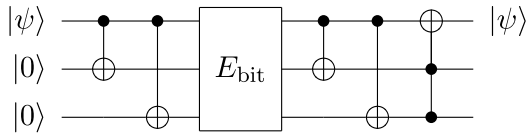
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.



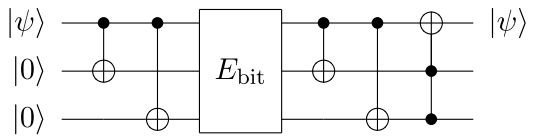
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.



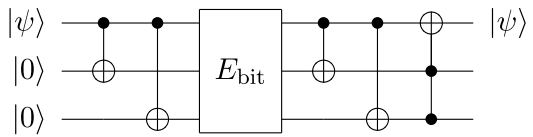
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.



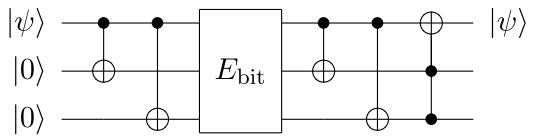
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:



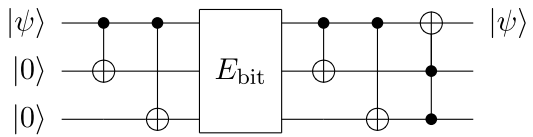
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.



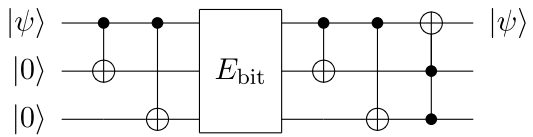
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.
  - Then $\langle\psi|P_1|\psi\rangle =$



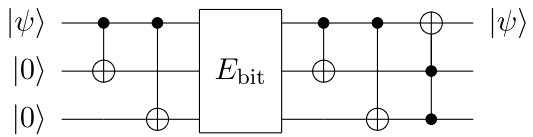
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.
  - Then $\langle\psi|P_1|\psi\rangle =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(|100\rangle\langle 100| + |011\rangle\langle 011|)(a|100\rangle + b|011\rangle) =$



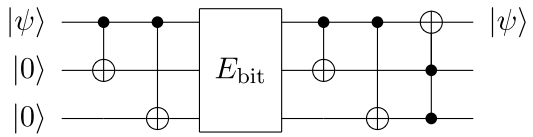
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.
  - Then $\langle\psi|P_1|\psi\rangle =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(|100\rangle\langle 100| + |011\rangle\langle 011|)(a|100\rangle + b|011\rangle) =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(a|100\rangle + b|011\rangle) = \overline{a}a + \overline{b}b = 1$



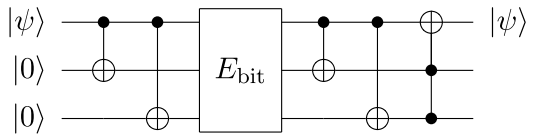
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.
  - Then $\langle\psi|P_1|\psi\rangle =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(|100\rangle\langle 100| + |011\rangle\langle 011|)(a|100\rangle + b|011\rangle) =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(a|100\rangle + b|011\rangle) = \overline{a}a + \overline{b}b = 1$
- Checkpoint: Verify that $\langle\psi|P_0|\psi\rangle = \langle\psi|P_2|\psi\rangle = \langle\psi|P_3|\psi\rangle = 0$



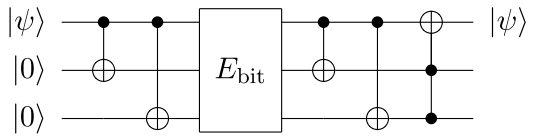
- Syndrome detection:
  - $P_0 \equiv |000\rangle\langle 000| + |111\rangle\langle 111|$: No error.
  - $P_1 \equiv |100\rangle\langle 100| + |011\rangle\langle 011|$: Bit flip on qubit one.
  - $P_2 \equiv |010\rangle\langle 010| + |101\rangle\langle 101|$: Bit flip on qubit two.
  - $P_3 \equiv |001\rangle\langle 001| + |110\rangle\langle 110|$: Bit flip on qubit three.
- Example:
  - Suppose there is an error at qubit one.
  - Then $\langle\psi|P_1|\psi\rangle =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(|100\rangle\langle 100| + |011\rangle\langle 011|)(a|100\rangle + b|011\rangle) =$
  - $(\overline{a}\langle 100| + \overline{b}\langle 011|)(a|100\rangle + b|011\rangle) = \overline{a}a + \overline{b}b = 1$
- Checkpoint: Verify that $\langle\psi|P_0|\psi\rangle = \langle\psi|P_2|\psi\rangle = \langle\psi|P_3|\psi\rangle = 0$
- After the measurement the state remains the same: $P_1|\psi\rangle = \Psi$.



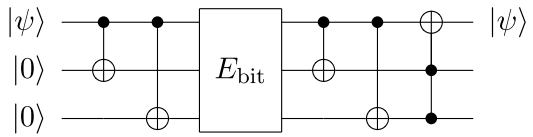
- Recovery: Use the value of the error syndrome to apply the appropriate recovering procedure.



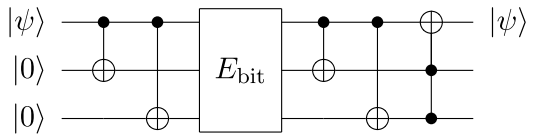
- Recovery: Use the value of the error syndrome to apply the appropriate recovering procedure.
  - 0: Do nothing.



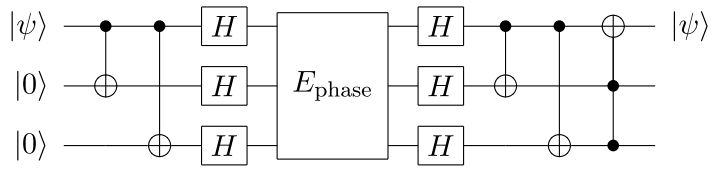
- Recovery: Use the value of the error syndrome to apply the appropriate recovering procedure.
  - 0: Do nothing.
  - 1: Flip qubit one.



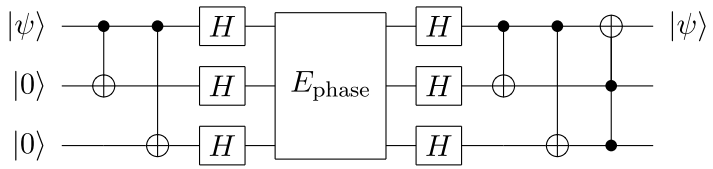
- Recovery: Use the value of the error syndrome to apply the appropriate recovering procedure.
  - 0: Do nothing.
  - 1: Flip qubit one.
  - 2: Flip qubit two.



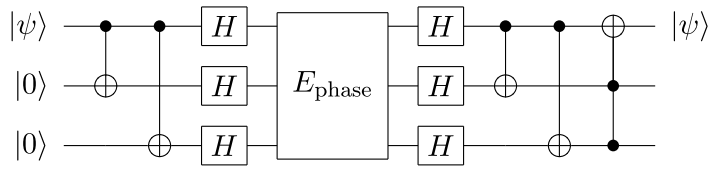
- Recovery: Use the value of the error syndrome to apply the appropriate recovering procedure.
  - 0: Do nothing.
  - 1: Flip qubit one.
  - 2: Flip qubit two.
  - 3: Flip qubit three.



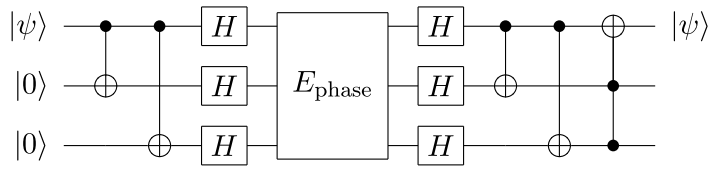
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$



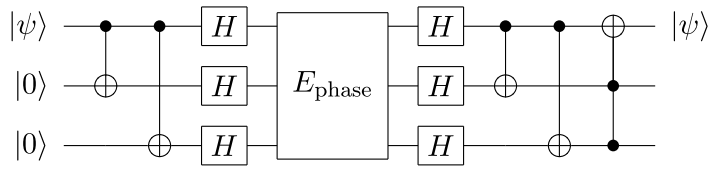
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre



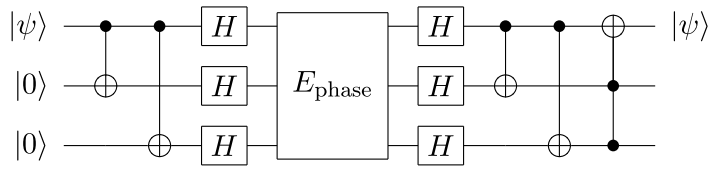
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre
- Writing things in the basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$...



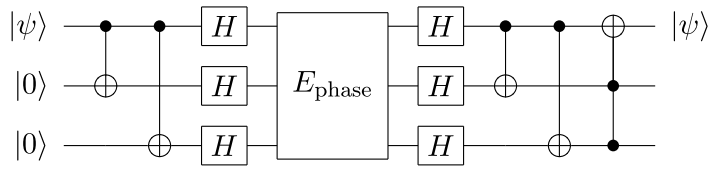
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre
- Writing things in the basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$...
- The operator Z acts as a bit flip with respect to $|+\rangle$ and $|-\rangle$.



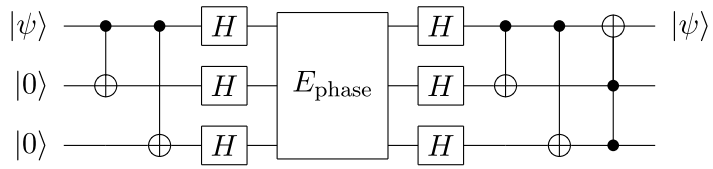
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre
- Writing things in the basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$...
- The operator Z acts as a bit flip with respect to $|+\rangle$ and $|-\rangle$.
- Logical Zero: $|0\rangle \equiv |+++\rangle$. Logical One: $|1\rangle \equiv |---\rangle$.



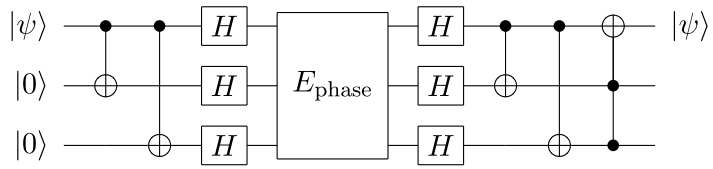
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre
- Writing things in the basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$...
- The operator Z acts as a bit flip with respect to $|+\rangle$ and $|-\rangle$.
- Logical Zero: $|0\rangle \equiv |+ + +\rangle$. Logical One: $|1\rangle \equiv |- - -\rangle$.
- How to achieve this? Using Hadamard Gates.



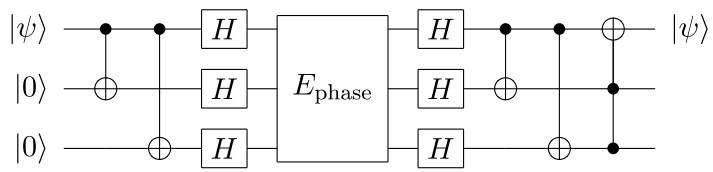
- Phase Flip Error: $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$
- A phase flip may be interpre
- Writing things in the basis $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$...
- The operator Z acts as a bit flip with respect to $|+\rangle$ and $|-\rangle$.
- Logical Zero: $|0\rangle \equiv |++\rangle$. Logical One: $|1\rangle \equiv |--\rangle$.
- How to achieve this? Using Hadamard Gates.
- First send $|0\rangle \rightarrow |000\rangle$ and $|1\rangle \rightarrow |111\rangle$. Then apply Hadamard $H^{\otimes 3}$.



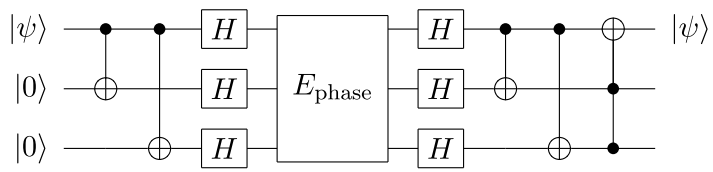
- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.



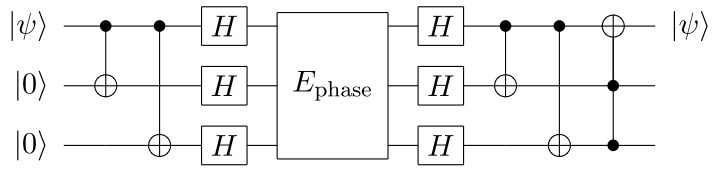
- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.
- Syndrome detection:



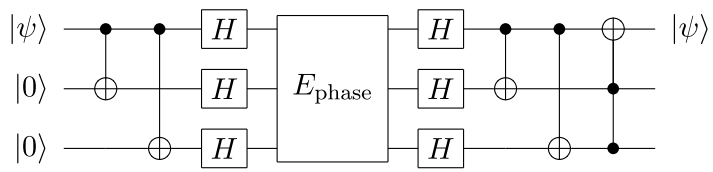
- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.
- Syndrome detection:
  - $P_0 \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$: No error.



- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.
- Syndrome detection:
  - $P_0 \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$: No error.
  - $P_1 \equiv |-++\rangle\langle-++| + |+--\rangle\langle+--|$: Phase flip on qubit one.



- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.
- Syndrome detection:
  - $P_0 \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$: No error.
  - $P_1 \equiv |-++\rangle\langle-++| + |+--\rangle\langle+--|$: Phase flip on qubit one.
  - $P_2 \equiv |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|$: Phase flip on qubit two.



- The syndrome projectors are analogous to those for bit-flip, except that they act in the basis $|+\rangle, |-\rangle$.
- Syndrome detection:
  - $P_0 \equiv |+++\rangle\langle+++| + |---\rangle\langle---|$: No error.
  - $P_1 \equiv |-++\rangle\langle-++| + |+--\rangle\langle+--|$: Phase flip on qubit one.
  - $P_2 \equiv |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|$: Phase flip on qubit two.
  - $P_3 \equiv |++-\rangle\langle++-| + |--+\rangle\langle--+|$: Phase flip on qubit three.

- Can protect againt the effect of an arbitrary error on a single qubit.

- Can protect againt the effect of an arbitrary error on a single qubit.
- First protect against phase flips: $|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$.

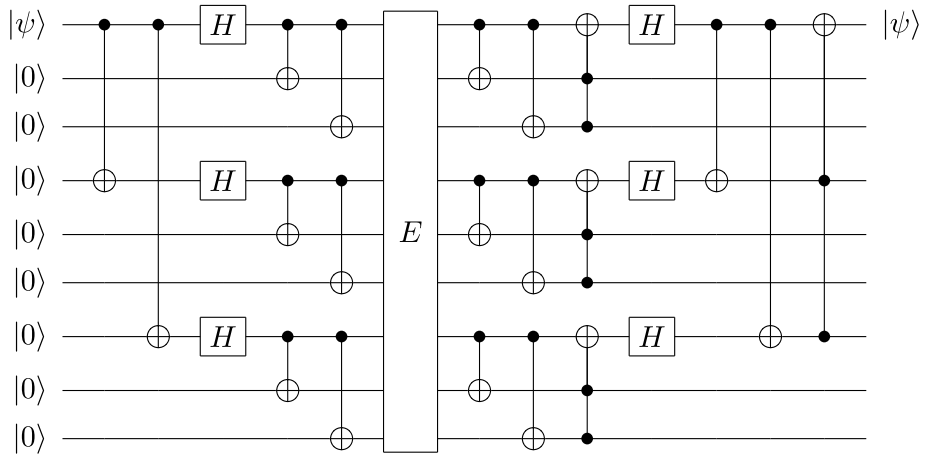
- Can protect againt the effect of an arbitrary error on a single qubit.
- First protect against phase flips: $|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$.
- Then protect each of the qubits against bit-flip. Encode

$$|+\rangle \rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}} \text{ and } |-\rangle \rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

.

$$|0\rangle \rightarrow \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$


$|\psi\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
H
H
E
H
H
H
$|\psi\rangle$

- The Shor code can correct over arbitrary 1-qubit errors.

- The Shor code can correct over arbitrary 1-qubit errors.
- $U = c_0 I + c_1 \sigma_x + c_2 \sigma_y + c_3 \sigma_z$.

- The Shor code can correct over arbitrary 1-qubit errors.
- $U = c_0 I + c_1 \sigma_x + c_2 \sigma_y + c_3 \sigma_z$.
- where

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

,

- A linear code C of length n over a field F is a subspace of F^n. Here we will consider that $F = \mathbb{Z}_2$.
- The words of the codespace F^n are vectors. Call them codewords.
- A linear code $C$is a $[n, k]$ code if C has dimension k.
- If C is a $[n, k]$ code then $|C| = |F|^k$. Thus we can consider that C encodes k bits of information into n qubits.
- The distance of the code is $d = min_{v,u \in C}\{i | v_i \neq u_i\}$
- Example: Repetition Code of length n over F.

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx
- Checkpoint what is the Generator matrix for the r repetition code?

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx
- Checkpoint what is the Generator matrix for the r repetition code?
- Parity check matrix H. A code is the set of n-bit vectors x such that $Hx = 0$. H is a $(n-k) \times n$ matrix.

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx
- Checkpoint what is the Generator matrix for the r repetition code?
- Parity check matrix H. A code is the set of n-bit vectors x such that $Hx = 0$. H is a $(n-k) \times n$ matrix.
- Since $Hy = 0$ for all codeword y, we have that $H(y+e) = He$

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx
- Checkpoint what is the Generator matrix for the r repetition code?
- Parity check matrix H. A code is the set of n-bit vectors x such that $Hx = 0$. H is a $(n-k) \times n$ matrix.
- Since $Hy = 0$ for all codeword y, we have that $H(y+e) = He$
- Dual code: $C^{\perp}$ such that generator matrix is H^T and parity check matrix is G^T.

- A linear code C encoding k bits into n-bits can be specified by a $n \times k$ generator matrix G whose elements are over $\mathbb{Z}_2$.
- G maps a k bit message x into the n-bit message Gx
- Checkpoint what is the Generator matrix for the r repetition code?
- Parity check matrix H. A code is the set of n-bit vectors x such that $Hx = 0$. H is a $(n-k) \times n$ matrix.
- Since $Hy = 0$ for all codeword y, we have that $H(y+e) = He$
- Dual code: $C^{\perp}$ such that generator matrix is H^T and parity check matrix is G^T.
- Equivalently: $C^{\perp}$ consists of all codewords y such that y is orthogonal to all codewords in C.

- Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ classical linear codes such taht $C_2 \subset C_1$ and such that both C_1 $C_2^{\perp}$ correct t errors.

- Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ classical linear codes such taht $C_2 \subset C_1$ and such that both C_1 $C_2^{\perp}$ correct t errors.
- Define a $[n, k_1 - k_2]$ quantum code $CSS(C_1, C_2)$ capable of correcting errors on t qubits.

- Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ classical linear codes such taht $C_2 \subset C_1$ and such that both C_1 $C_2^{\perp}$ correct t errors.
- Define a $[n, k_1 - k_2]$ quantum code $CSS(C_1, C_2)$ capable of correcting errors on t qubits.
- called the CSS code of C_1 over C_2.

- Let x be any codeword in C_1.

- Let x be any codeword in C_1.
- $$|x \oplus C_2\rangle \equiv \frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle$$

- Let x be any codeword in C_1.
- $$|x \oplus C_2\rangle \equiv \frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle$$
- If $x' \in C_1$ is such that $x' - x \in C_2$ then $|x \oplus C_2\rangle = |x' \oplus C_2\rangle$

- Let x be any codeword in C_1.
- $$|x \oplus C_2\rangle \equiv \frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle$$
- If $x' \in C_1$ is such that $x' - x \in C_2$ then $|x \oplus C_2\rangle = |x' \oplus C_2\rangle$
- If x and x' belong to different cosets then $|x \oplus C_2\rangle$ and $|x' \oplus C_2\rangle$ are orthonormal.

- Let x be any codeword in C_1.
- $$|x \oplus C_2\rangle \equiv \frac{1}{|C_2|} \sum_{y \in C_2} |x + y\rangle$$
- If $x' \in C_1$ is such that $x' - x \in C_2$ then $|x \oplus C_2\rangle = |x' \oplus C_2\rangle$
- If x and x' belong to different cosets then $|x \oplus C_2\rangle$ and $|x' \oplus C_2\rangle$ are orthonormal.
- Dimension of $CCS(C_1, C_2) = |C_1|/|C_2| = 2^{k_1 - k_2}$, and thus $CSS(C_1, C_2)$ is an $[n, k_1 - k_2]$ quantum code.

- Bit flip vector: e_1

- Bit flip vector: e_1
- Phase flip vector: e_2

- Bit flip vector: e_1
- Phase flip vector: e_2
- If $|x + C_2\rangle$ was the original state, then the corrupted state is $\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x + y + e_1\rangle$

- Bit flip vector: e_1
- Phase flip vector: e_2
- If $|x + C_2\rangle$ was the original state, then the corrupted state is $\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x + y + e_1\rangle$
- Detection of where the bitflip occurred: $|x \oplus y \oplus e_1\rangle|0\rangle \rightarrow |x \oplus y \oplus e_1\rangle|H_1(x + y + e_1)\rangle = |x + y + e_1\rangle|H_1 e_1\rangle$

- Bit flip vector: e_1
- Phase flip vector: e_2
- If $|x + C_2\rangle$ was the original state, then the corrupted state is $\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x + y + e_1\rangle$
- Detection of where the bitflip occurred: $|x \oplus y \oplus e_1\rangle|0\rangle \rightarrow |x \oplus y \oplus e_1\rangle|H_1(x + y + e_1)\rangle = |x + y + e_1\rangle|H_1 e_1\rangle$
- this last equality follows from the fact that $x + y$ is eliminated by the parity matrix

- Bit flip vector: e_1
- Phase flip vector: e_2
- If $|x + C_2\rangle$ was the original state, then the corrupted state is $\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x + y + e_1\rangle$
- Detection of where the bitflip occurred: $|x \oplus y \oplus e_1\rangle|0\rangle \rightarrow |x \oplus y \oplus e_1\rangle|H_1(x + y + e_1)\rangle = |x + y + e_1\rangle|H_1 e_1\rangle$
- this last equality follows from the fact that $x + y$ is eliminated by the parity matrix
- Thus the state becomes

$$\frac{1}{\sqrt{C_2}}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x + y + e_1\rangle|H_1 e_1\rangle$$

- Error detection: Measure the ancila register obtaining $|He_1\rangle$

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle$$

- Error detection: Measure the ancila register obtaining $|He_1\rangle$

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle$$

- Knowing the error syndrome $H_1 e_1$ one can infer e_1 since C_1 corrects up to t errors.

- Error detection: Measure the ancila register obtaining $|He_1\rangle$

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x+y+e_1\rangle$$

- Knowing the error syndrome $H_1 e_1$ one can infer e_1 since C_1 corrects up to t errors.
- Error Correction: Simply apply NOT gates to the qubits at whichever the positions a flip occurred.

$$\frac{1}{|C_2|}\sum_{y\in C_2}(-1)^{(x+y)\cdot e_2}|x+y\rangle$$

- Detecting Phase Flips: Apply H to each qubit.

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

- Detecting Phase Flips: Apply H to each qubit.

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

- Set $z' = z + e_2$

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} |z' + e_2\rangle$$

- Detecting Phase Flips: Apply H to each qubit.

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

- Set $z' = z + e_2$

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} |z' + e_2\rangle$$

- Exercise: If $z' \in C_2^{\perp}$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$ and if $z' \notin C_2^{\perp}$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$.

- Detecting Phase Flips: Apply H to each qubit.

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot(e_2+z)} |z\rangle$$

- Set $z' = z + e_2$

$$\frac{1}{\sqrt{|C_2| \cdot 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)\cdot z'} |z' + e_2\rangle$$

- Exercise: If $z' \in C_2^{\perp}$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2|$ and if $z' \notin C_2^{\perp}$ then $\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$.
- The state becomes:

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^{\perp}} (-1)^{x \cdot z'} |z' + e_2\rangle$$

- This is just like a bit flip error e_2. Apply the parity check H_2 as before to get e_2 and correct it likewise:

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^{\perp}} (-1)^{x \cdot z'} |z'\rangle$$

- This is just like a bit flip error e_2. Apply the parity check H_2 as before to get e_2 and correct it likewise:

$$\frac{1}{\sqrt{2^n/|C_2|}} \sum_{z' \in C_2^{\perp}} (-1)^{x \cdot z'} |z'\rangle$$

- Apply H to each qubit obtaining:

$$\frac{1}{|C_2|} \sum_{y \in C_2} |x \oplus y\rangle = |x \oplus C_2\rangle$$